? t s12/9/136

12/9/136 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01801703 SUPPLIER NUMBER: 17162680 (THIS IS THE FULL TEXT)
Toward electronic money: some Internet experiments. (includes related articles on RSA's public-key encryption and on smart cards for digital money)
Dyson, Peter E.
Seybold Report on Desktop Publishing, v9, n10, p3(9)
June 10, 1995
ISSN: 0889-9762 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 6493 LINE COUNT: 00607

TEXT:

In the real world, "money" covers a wide range of financial instruments with varying degrees of acceptance, anonymity, safety, speed, and so on. The list includes currency, checks, traveler's checks, credit and debit cards, bank letters of credit, bearer bonds, gold coins, bank wire transfers, company-store scrip and many more. None of these_not even cold cash_is suitable for every commercial purpose.

Now that millions of corporate and personal computers are connected by the Internet, new business opportunities are raising the demand for a new form of money that works well in the wired world. It is not yet clear just what this form will be, but several approaches have been proposed and some experiments are already under way. In this article, we will look at how digital money might be implemented and examine four representative systems that span the range of alternatives.

In The Rub!iyat of Omar Khayy!m, the poet muses

I often wonder what the vintners buy
One half so precious as the stuff they sell.

What publishers have to sell is an intangible commodity: information. Money, as any economics textbook will tell you, is also an intangible thing; at bottom, it is the trust that having received it, you will later be able to spend it. Until recently, information has been created on paper and packaged as tangible objects: books, newspapers, and so on. It has thus seemed natural to be paid in the form of other objects: paper money, credit cards, etc. With the rise of systems that deliver information electronically, it is appropriate that payment should also take an electronic form.

The best money

Creating and maintaining trust is the ultimate purpose of all digital money schemes. To that end, any system must have certain features, although the strength of these features may vary and some features are diametrically opposed to others. In the following section (which is regrettably rather general and theoretical), we will use the term "token" to mean any digital message that purports to be a form of money. The ideal token would be: Accessible. The mechanisms that are used to create, transmit and receive tokens must be convenient and quick.

Authentic. Users must be assured that the tokens they accept are valid. This assurance might involve contacting some third-party authority that can certify the tokens, or it might involve some hardware device, such as a smart card.

Fungible. To be accepted as real money, tokens must be convertible into cash, or at least into bank balances that can be turned into cash.

Nonrefutable. Users must be able to verify, through some proof-of-payment mechanism, that a transaction has actually taken place. This might be done by adding information to the token itself (like endorsements on the back of a paper check) or by a separate receipt document (which itself must be accessible, authentic, private, and so on).

Private. The system must keep confidential any records of

transactions. In some systems, privacy and nonrefutability are incompatible; but at least one proposal offers both features.

Protected. Users must be assured that they cannot be swindled or falsely accused of attempting to swindle. Note that protection may require some loss of privacy, such as when settling a claim of fraud or tracking down a counterfeiter.

Reliable. The infrastructure that handles tokens must be available all the time; it must work even with heavy system loads or component failures.

Options. Beyond these basic properties, there are several features that might or might not be important to a digital-token system. For example:

Cash purchase. Should users be allowed to buy tokens for cash_that is, anonymously? This would let people without bank accounts use tokens, but it would provide yet another mechanism for laundering the profits of crime.

International conversion. Should a token purchased with one currency (say, Dutch guilders) be cashable in a different currency (such as U.S. dollars)? Electronic communication would allow instantaneous determination of exchange rates, but there could be interesting impacts on national currency-control and banking laws.

Traceability. To prevent forgery, tokens might bear unique serial numbers that are assigned from a central registry. That would make it easier to spot duplicate tokens_which, after all, are merely strings of bits_and track down criminals or broken cash dispensers, and it might simplify the nonrepudiation process. But it could also strip away the privacy of transactions.

Maximum rate limits. To reduce the risk of crime or software failure, transaction systems could be programmed to limit the amount of money that can be transferred in any hour or day.

Implementation issues. Even if agreement were reached on all of the above issues, there would still be a host of questions to settle. Here are just a few.

Issuers. Who creates tokens? Traditionally, governments have reserved the right to issue currency. But banks also create money by extending credit_and thus, indirectly, individuals create money when they use credit cards.

Similarly, who is obliged to accept tokens? Traditionally, one way governments validate their currency is by accepting it as payment of taxes. Banks validate the credit-based money they create by accepting checks and wire transfers for deposit in cash accounts.

Liability. If an electronic token is lost, stolen or counterfeited, who suffers the loss? This question is one of the most prominent differences among the other forms of money. For example, there is no recourse if cash is lost, while traveler's checks are guaranteed against loss and forgery by the issuing bank. Under U.S. law, the cardholder is liable for only the first $50 charged to a stolen card; the issuing bank is liable for the rest of the loss. We suspect that several forms of digital money will likewise be offered with a variety of guarantees and liabilities.

Accounting, fees and floats. For how long should transaction records be maintained, and what accounting standards will apply to the handling of digital money? Should fees be charged on the creation of tokens or on each transaction? Should fees be payable in cash or merely deducted from the value of the tokens? Should tokens be created in fixed denominations? If so, how do you make change? If tokens are created and stored until spent, who keeps the interest that is earned on the unspent balance?

Whom can you trust? Encryption, and particularly public-key encryption, is the underlying technology for nearly all the proposals for digital money. But encryption by itself cannot create trust. It can only transfer distrust. For example, it is said that a public-key signature can unambiguously verify the identity of the sender of a message. But that presumes that the public key truly identifies the right person. You must then ask how trustworthy is the source of public keys. Or, as the Romans long ago wondered, quis custodet ipsos custodes; who will guard the guardians?

In all of the following proposals, there is some mechanism for

certifying whether a given token is valid. Typically, this is a trusted third party that specializes in performing certifications. Typically, such a certification authority will guarantee its work by accepting the liability if it somehow fails. Like any well-run business, the authority will back up its guarantee by passing the buck and purchasing an insurance policy.

Someday, we think, a single digital-money system might emerge from today's experiments. If that happens, it is unlikely that there could be a single certification authority. To satisfy the needs for speed, failure resistance and national parochialism, we think there must be many certification authorities. That, in turn, suggests that there might have to be a higher authority that can certify the local authorities, and perhaps an entire hierarchy of such certification authorities. But the buck must stop somewhere. Ultimately, every financial system is based on blind faith.

CommerceNet, Netscape: ordinary credit

Two companies, CommerceNet and Netscape Communications, have staked their reputations on secure transmission of credit-card numbers. Although their approaches differ in detail, both are extending the reach of today's credit- card system to the Internet without making any change in the underlying financial mechanism. Thus, anyone who has a credit card and a secure Web browser can do business with any merchant that accepts cards and operates a secure server. In today's Internet, which is for the most part still a playground for the technocracy, access to credit can be taken for granted and will not be a limitation for either CommerceNet or Netscape.

CommerceNet's CyberCash. To use CommerceNet's system, you must install the CyberCash Web-browser software on your pc. (Currently, the software is available only for Windows; you can get it from http://www.cybercash.com.) In addition to the standard features of most browsers, it displays a Pay button when you are in contact with a server that supports the Secure Hypertext Transport Protocol (s-http).

In a typical transaction, you examine a merchant's online ad for some product (typically a document that can be downloaded), and if you agree to the price, you press the Pay button. Your pc sends a message to the merchant's server to start the transaction, and the merchant responds by sending you an electronic invoice. You enter your name, credit-card number and expiration date in the marked spaces on the invoice form, and send it back to the merchant.

The completed invoice is then encrypted and sent back to the merchant. The merchant adds his own identification codes and forwards the invoice to CommerceNet's CyberCash server. The server decrypts the invoice and contacts the appropriate credit center to obtain an authorization code. If the card number is approved, CommerceNet sends an ok signal to the merchant, which proceeds to deliver the goods to you.

CommerceNet, meanwhile, posts the credit transaction, adding the sale to the merchant's account and charging your credit card through the normal banking system. A similar procedure would be used to void a sale and post a refund.

CyberCash checking. The above system is thus misnamed; it is really a CyberCredit system. But CommerceNet has also developed_though not widely deployed_a system for conducting electronic cash-like transactions between individuals. The individuals must have CyberCash accounts, which work rather like numbered Swiss bank accounts. Upon receipt of a properly encrypted message, the CyberCash server will transfer funds from one numbered account to another. The server only needs to know the amount and the two account numbers; it does not need any other information about the who or why of the transaction. Thus, like real cash, CyberCash is anonymous and private. Also like real cash, there is no float from funds in transit within the CyberCash system, for transfers are instantaneous. Nor is there any interest earned on account balances. Finally, you can transfer money into your CyberCash account from a bank account and you can withdraw money by transferring it to a bank account.

CommerceNet's encryption. Within the cryptographic community, CommerceNet has incurred some scorn for refusing to divulge its encryption technique. CommerceNet says only that parts of its system use the U.S. government-approved Data Encryption Standard (des, which relies on 56-bit

keys) while other parts draw on RSA's public-key encryption (see p. 9). To professional cryptographers, this smacks of a "security through obscurity" strategy. Cryptographers have learned not to put their faith in any scheme that cannot be proven secure by mathematical analysis.

Netscape's one-time keys. Built into every copy of the Netscape Navigator is an encryption system called the Secure Sockets Layer (ssl). When an ssl- equipped browser is in communication with an ssl-equipped server (such as the one Netscape sells), their communication can be carried on in secrecy. It thus allows sending credit-card numbers and other sensitive information over the Internet.

In ssl, Netscape uses RSA's public-key technology in an interesting way. Whenever it begins a secure data transfer, the Netscape browser generates a "secret token"_a large, randomly chosen prime number_that will be the encryption key for that session. The browser then needs to send this token to the other party (the ssl-compliant server) in secrecy. To do so, the browser contacts RSA's key server (there is only one, so far) to learn the server's public key. It encrypts the token with the public key and sends it over the Internet; the ssl server uses its private key to extract the token, and thereafter the two computers use the token for their encryption. At the end of the data transfer, the token is discarded.

The advantage of a one-time token such as this is that it makes relatively little use of the RSA encryption process. Public-key encryption is very strong, but it takes a lot of number crunching. Netscape has chosen to do most of its communication with an encryption algorithm that is theoretically weaker but runs fast, even on a '486 processor. It then shores up the weakness of its algorithm by using each token for only a short time. In theory, an enemy could break the code by examining a sufficient quantity of encrypted data. Netscape makes sure that the amount of data sent over the wire is relatively small. And even if someone were to break the code once, he'd have to start all over the next time, because you would be using a different key.

What we have so far described solves only half the security problem. Before sending your credit-card number into the ether, you might want some assurance that the server is legitimate. To do so, your browser asks the server to give you an identifying message that is encrypted with its private key. You can then obtain the public key and read the message, or you can send the message to RSA's server, which will respond with a certificate (a digital yea or nay). The latter is the method that Netscape has put into its browser.

Netscape browsers make no effort to prove their identity to servers, however. It would be possible to use the same technique as above, but that would require obtaining a pair of RSA keys for every browser. Currently, RSA charges a few hundred dollars per year for key-certification services. Merchants will find this a small price, but it is more than consumers are likely to pay. However, the merchant does not really need to certify the browser's identity; he only needs to verify that your credit card is good, and that can be done by conventional means.

Netscape also hastens to point out that its algorithms have been published and thoroughly scrutinized by independent experts.

Prospects. Until recently, the technical differences between CommerceNet's s-http and Netscape's ssl meant that the two systems were doomed to incompatibility. Last month, though, Terisa Systems announced that it will develop a programmer toolkit that combines the two technologies. As Terisa's work is incorporated into browsers and servers and percolates into the market, the compatibility problems should go away. That, in turn, may ease market acceptance of secured credit-card transactions over the Internet.

Analysis. Regardless of technical improvements, the credit-card approach has a fundamental limitation: The cost of processing a credit transaction today is substantial. Thus credit cards are not suitable for tiny transactions. Yet if electronic commerce is to become widespread, many transactions must be priced in pennies. For example, you might balk at paying a dollar to read one comic strip, yet be happy to pay a nickel.

One reason that credit cards are so expensive is that the banks must cover their losses from lost and stolen cards, fraud and human error. Much

effort has gone into designing bulletproof systems of all-digital money, which theoretically would avoid most such risks.

Another problem is that neither Netscape nor CommerceNet offers any better privacy than today's credit cards. This is acceptable now, but it might not be in the near future. One good scandal would send customers running for the exits.

No one has yet proposed a scheme for e-cash that is simultaneously private yet traceable, freely spendable yet loss-proof, cheap to implement yet feature rich. Nevertheless, people are trying, and we think that sooner or later some such scheme will work well enough that it becomes a standard for Internet transactions. When that happens, credit cards will start to play a much smaller role than they necessarily do today.

First Virtual: aggregating transactions

The great virtue of First Virtual Corporation's online transaction system is that it is a working system; it has been up and running for more than half a year. Although it uses the Internet for transactions, it operates without any encryption schemes. The only special software it requires a customer to have is a Web browser with forms capability. Rather than trying for impregnable security, First Virtual keeps credit-card numbers off the Internet. Beyond that, the merchants who participate in the FV scheme simply acknowledge and accept a certain level of risk.

Signing up. Before you can do business through First Virtual, you must register as a customer. The process is simple enough: Using a forms-capable Web browser, fill in the registration form transmitted by FV's server. On this form, you are asked to make up your own account identifier, which will identify you to the system in all subsequent activities.

In picking your identifier, FV suggests that you choose a sequence of letters and numbers (up to 24 characters long) that you can remember; it should be sufficiently idiosyncratic, however, that no one else is likely to think of it. FV further instructs you not to include in the sequence any reference to your credit-card numbers, passwords or other sensitive information. This is because the identifier is not a secret; it will be transmitted over the Net in the form of plain text every time you buy something. That would appear to expose you to some risk; but as we shall see, the FV system minimizes that risk.

Sometime after you have returned the electronic form, you must give FV your credit-card information. This step, however, is handled offline: you call FV's toll-free phone number and enter your card number via your phone's keypad. Clearly, this is not a risk-free step; phones can be tapped, clerks can be corrupted, and so on. But the risk is no different than any other credit-card purchase over the phone, and that is something that millions of people do every day.

There is a sign-up charge of $2, and every time you instruct FV to change your account information (e.g., new card number or expiration date) there is a further $2 charge. However, that is the only overhead cost that you bear. First Virtual makes its money on the transaction fees its member merchants pay.

Transactions. Now that you have an account, you can go shopping. Some of First Virtual's participating merchants rent disk space on FV's InfoHaus server, while others have their own servers. When you have found a document you want to buy, you supply your account identifier to the merchant via a screen form.

The merchant may, if he wishes, send a quick query to First Virtual's credit computer to ascertain that your account identifier is valid. (Your privacy is protected here, because the only information FV will provide is a simple yea or nay. The merchant does not obtain your credit-card number or even your real name.) Then the merchant transmits the document to you, either by attaching it to an e-mail message or by granting access so your Web browser can download the file.

The merchant then sends FV a notice of the sale. The notice includes your account identifier, the merchant's own account identifier, the price of the goods (and the unit of currency in which the price is stated) and a brief description of the goods. However, the sale is not yet complete. The FV **computer** **sends** you an e-mail message asking you to **confirm** the **transaction** . In your reply, you may **send** one of three possible

responses:

Yes. You have inspected the information and you wish to keep it. First Virtual charges the stated price to your credit card. It then pays the merchant, after deducting a transaction fee.

No. After looking the product over, you have decided that it really isn't what you wanted. You decline to pay, and are now honor bound to erase the information from your system. The merchant gets nothing.

Fraud. Someone else has used your account identifier. First Virtual immediately closes that account. Again, the merchant gets nothing.

If you fail to respond to the confirmation message within a few days, First Virtual tries again. After several failures, it assumes that your account has become inaccessible (perhaps you have gone on vacation or your computer has broken) and suspends your id until you do respond.

Becoming a merchant. Selling information through First Virtual is straightforward. You must open an account and establish an identifier, exactly as a buyer would. In fact, the same account can be used for buying and selling. The main difference is that a merchant must also designate a checking account into which First Virtual will deposit the proceeds of any sales. (Currently, this checking account must be with a U.S. bank. For overseas vendors, FV provides an instruction sheet on opening such an account.) As a merchant, you have the option of renting space on the FV server, known as the InfoHaus, for which FV will charge you $1.50 per megabyte per month plus 8% of your transaction revenues. (At least, it plans to make such a charge eventually. During the current start-up period, FV is waiving the charge.) Alternatively, you may operate your own server. FV has published the server transaction protocol, which it calls the Simple Green Commerce Protocol, or sgcp. In addition, it offers free software that you can integrate with your system: either scripts for the common gateway interface (cgi) used in most Web servers or c libraries for e-mail and ftp servers.

There are three components to each document that you offer for sale: the title and price; a free description or a sample of the contents; and the document itself. (Note that we are using the word document to cover any bundle of information: a research paper, a recipe collection, a video clip, an executable program, etc.) Generally, customers will find the title in a listing or catalog, request the description and then (perhaps) order the document.

As a merchant, you can set any price you want for your goods. However, because First Virtual deducts transaction fees from your sales, the effective minimum price per transaction is $0.31. If you want to charge less per item, you have to sell the items in batches so the total price of the transaction is greater than 31 cents. There is a maximum price, too: $999,999.99; but we doubt this will be restrictive for most publishers.

The fee structure is simple: Each transaction costs the merchant $0.29 plus 2% of the value of the sale. (This is where the 31-cent minimum comes from.) For example, on a $20 sale, First Virtual charges the customer the stated $20 price. It then takes out its $0.29 base fee plus $0.40 (that is, 2% of $20), and credits the merchant with $19.31.

In addition, each time First Virtual makes a deposit to the merchant's checking account, it charges $1 as a processing fee. Because each deposit typically covers several days' worth of sales, this is not a serious burden. Each time it makes a deposit, FV e-mails a notification message to the merchant; for security, the checking-account number is not disclosed in the message.) Overall, the FV cost structure is less than what most banks charge for processing credit-card sales.

Risk management. In the First Virtual scheme of things, the merchant bears nearly all of the risk. He must deliver his product in hopes that it will be paid for; First Virtual only pays the merchant after it has received payment from the customer. If the customer declines the sale or claims fraud, if the customer's credit goes sour, or if the customer later disputes First Virtual's billing, the merchant gets nothing.

On the other hand, the merchant's risk is actually less than that of most other information publishers. The "manufacturing cost" for one copy of the information is close to zero, and there are no returns, repairs or refunds to deal with. Some customers may pass along copies to their

colleagues, but that problem is no different from the usual issues of photocopying or software piracy.

There are some defenses against cheating, moreover. First, each customer is advised that he has only one chance to reject a sale; if he accepts it via the e-mail confirmation message, he will be held to his commitment. If he later refuses to pay the credit-card bill, First Virtual closes his account. Each merchant is encouraged to monitor the activity on his own server and is allowed to refuse service to anyone suspected of abusing the system. First Virtual also monitors the activity in each account, and if a customer declines too many purchases (based on a formula that First Virtual declines to reveal), he may find his account summarily suspended.

Offsetting the merchant's risk is the opportunity to reach a wider market_which, for some kinds of specialized information, means the opportunity to be in business at all. Because the customer bears little risk of disappointment, he is likely to sample a wider range of information products. And because sales are handled by automated servers, gratification is nearly instantaneous (give or take the time to download a file or receive an e-mail attachment), and the store can stay open around the clock.

In theory, FV merchants could sell tangible goods as well as information. However, First Virtual discourages this. If a defect turns up in an information product, the vendor can simply transmit a fresh copy (for garbled files) or perhaps promise to fix the bug "real soon." Defects in hard goods, though, are costly and time-consuming to remedy, leading to greater customer dissatisfaction. A customer who is annoyed enough may exercise his ultimate sanction and repudiate the credit-card charge, which will cause First Virtual to retaliate by closing his account_an unhappy outcome for all concerned. Analysis. Although it is based on ordinary credit cards, First Virtual has placed itself in the role of an intermediary that aggregates small transactions (hence lowering costs) and partially shields a customer's privacy. It remains to be seen how low First Virtual can drive its costs, but it has every incentive to do so.

Although customer privacy is not absolute in First Virtual's system, it is no worse_and in most cases it is much better_than any other credit-card transaction today, such as in a store or over the telephone. Merchants can learn very little about their customers beyond their account identifiers and (possibly) their e-mail addresses, unless the customer voluntarily discloses the information. In experimenting with the system, we found that some merchants are nosy and require the customer's real name and address before closing a sale, but many are content with getting paid anonymously.

First Virtual itself necessarily accumulates a fair amount of information about its customers: where they shop, how much they spend and, to some extent, what they are buying. (The transaction description that the merchant sends to First Virtual may be vague, but it has to contain enough information that the customer can approve the confirmation e-mail message.) Again, however, this is no more than any other credit company can gather.

DigiCash: inherent privacy

There is a substantial body of opinion in the online community that the ultimate goal for electronic commerce must be a form of digital cash. Besides the virtues of low cost and wide acceptance, such digital cash would also be anonymous and hard to forge, just like real cash. Thanks to public-key encryption, this is now a realistic option.

The DigiCash Corporation has developed such a scheme and has demonstrated a prototype of the technology. A large-scale test of the concept and the initial software has been in progress on the Internet since early January 1995. The CyberBucks used in the experiment are not intended to be convertible into any real currency. Nevertheless, several thousand people have signed up to be testers and received a grubstake of 100 CyberBucks. Buying and selling of information among the testers, along with some online games of chance, have been ongoing since the project started.

Minting a digital coin. The theory behind DigiCash's technology has been published in the August 1992 issue of Scientific American. It assumes that the cost (in waiting time and compute power) of the necessary

encryptions and transmission is very small_an assumption that is increasingly reasonable_so that electronic money can be created in fairly small denominations. For this reason, and to convey the notion that it is a distinct parcel of value, each unit of electronic money is often called a digital coin.

A digital coin begins its life when it is created by a bank. It is merely an electronic message that has been encrypted with one of the bank's private keys. The bank might use one key for one-dollar coins, another for five- dollar coins and so on. The bank would, of course, publish the corresponding public keys, allowing anyone to verify the value of such a coin. When the Pay button for an Internet purchase is pressed, your computer contacts the bank and asks to download some digital coins.

For each coin, your computer generates a large random number, which will act as the coin's serial number. In the event of fraud, this number can be revealed to stop a perpetrator from cashing your coin, so your computer must maintain a list of serial numbers for a reasonable amount of time. However, for privacy, you do not wish the bank to maintain a list of your serial numbers; if it did, it could easily discover where you spend your money. To prevent this, your computer will first encrypt each serial number with another random number. Then it applies your digital signature (encrypts the combined number with your private key) and sends the message to the bank.

The bank first verifies and removes your signature by decrypting the message with your public key. It does not bother to examine the serial number you supplied, because it knows that number is encrypted. It then debits your bank account and applies one of its own signatures corresponding to the size of the coin you have requested. The message is then sent back to you (perhaps encrypted with your public key to assure that only you can receive it). Before you spend the coin, you first remove the random number to restore your original serial number1.

To spend your money, you transmit the coin to another person. He verifies the bank's signature to be sure he's getting the right amount and then deposits the coin in the bank. (For simplicity, we will speak of a single bank; but just as in today's economy, there could be multiple banks with clearinghouses to settle accounts.) The bank accepts the coin because it recognizes its own signature. But it cannot connect the coin that you originally requested with the coin that it has just received, and so it cannot keep track of how you are spending your money.

Dealing with problems. The system thus protects your financial privacy. On the other hand, if you need to (for example, if you pay for an online movie and halfway through it, the movie server fails), you can reveal your serial number. The bank can then trace the coin and cancel payment. This presumes that the coin is deposited at once, rather than passing from computer to computer like metal coins. In the DigiCash experiment, coins are used only for a single transaction.

To protect itself against honoring a coin that has previously been used, the bank might keep a list of the serial numbers that it has already received. This protection is not perfect because each bank customer is allowed to make up his own serial numbers; there is no central registry. However, because the serial numbers are chosen randomly from a very large pool of numbers, the odds of two customers picking the same one are slim. The real problem is that over time, the list of coins that have already been spent will grow very large.

One solution is to put a time limit on the life of a digital coin. The chance that you will lose money when a coin expires is small, because you would rarely want to keep it more than a few seconds. Your computer would not generate the coin until you pressed the Pay button, and the whole process of downloading the coin from the bank, sending it to the vendor and then depositing it in the vendor's account would all happen at wire speed. The developers of DigiCash have proposed a method that purports to solve the problem in a more elegant way. When you pay a merchant, he (that is, his computer) generates a numeric query about each coin. Your computer's answer does not contain enough information to identify you, but the answers to two different queries about the same coin_which you would get if you spent a coin twice_would reveal enough information to allow tracing the

coin to your bank account. This method is not part of the current CyberBucks experiment, but it might be used in future trials.

Analysis. The DigiCash experiment is not directly comparable to CommerceNet or First Virtual because it is not tied to the real financial system. However, it seems clear that as the cost of computing continues to fall dramatically, the costs of the various encryptions and lookups that DigiCash requires will become negligible. If a real-world experiment with e-cash that is fully convertible into legal tender were conducted, most of the cost would probably occur at the point of conversion; money within the system would move at very low cost.

As to privacy, DigiCash provides very strong isolation of fund flows and, thus, gives effective financial privacy unless the individual chooses to disclose his actions. As we shall describe below, there is more to commercial privacy than this, but it is a start.

Becoming more anonymous

As described above, in a true digital cash system a bank cannot associate the money you have spent with the money a vendor has earned and deposited. However, the transaction is not completely anonymous, because the vendor would have to know your Internet address to transmit the information you had purchased. There is no perfect way around this, but it is possible to establish a network pseudonym that can preserve your privacy most of the time. This is done through the use of a forwarding agent.

A forwarding agent is a server that knows, but promises not to disclose, both your real Net address and your pseudonym, which is based on the server's Net address. When you want to transmit a message to a vendor, you package it inside a "digital envelope" specifying the message's ultimate destination and send the envelope to the forwarding agent. The agent removes your original Net address and substitutes the pseudonym, then passes the message along. Likewise, when the agent receives a message directed to your pseudonym, it looks up your real Net address and forwards the message.

Such a service allows you to present a persistent and stable persona to the world, and thus preserves many of the advantages of using your real name. For example, you might qualify for discounts based on volume. The merchant, for his part, would be able to maintain a blacklist of customers who have caused trouble in the past. At the same time, under normal conditions, no one would be able to assemble a complete dossier on you. Nevertheless, your privacy is not absolute, because a court order could force the forwarding agent to disclose your real identity.

Techniques for truly unbreakable anonymity have been described in the literature of cryptography. We are not aware of any financial system that uses such techniques now, but we think that eventually one or more of them will emerge into the marketplace. We suspect, though, that pure anonymity will turn out to be only a minor aspect of electronic commerce. The bulk of the Internet's transactions will be shielded by protections that are less than impervious because low cost will usually be a more important factor. Merely knowing that full privacy is available when we need it will satisfy most of us.

Conclusion

The examples we have detailed above are only a few of the proposals, alliances and experiments now taking place in the electronic commerce arena. We chose them because they represent the range of possibilities, not because we think these are most likely to succeed. In fact, in the computer industry, the early pioneers have often lost out to the later arrivals, who learned from the pioneers' mistakes and more precisely targeted their markets.

We have no doubt that some form of digital money will gain widespread use. In all likelihood there will be several alternative forms of digital money, each best at meeting some need, just as cash, checks, wire transfers and credit cards all meet different needs now. (Incidentally, we do not think that digital money will replace these other forms, any more than we think that screens will replace books anytime soon.) But the greatest need is for a cheap, fast, convenient and safe medium of exchange that can be used to buy very small units of information at low prices over the Internet.

Price. The public has always preferred an adequate and cheap solution to a better but slightly more expensive solution. We doubt that electronic money will be any different. Whoever offers the lowest transaction cost_including the intangible costs of inconvenience and delay_will win the game.

The systems that are currently active are based on credit cards, whose direct transaction costs range from $0.20 to $0.50 per purchase. Last winter, though, Visa and Carnegie Mellon University announced a system called NetBill, whose goal is to permit efficient selling of documents priced at $0.10. That, in turn, means the transaction cost must be less than $0.01. If CMU can achieve that goal, can operations such as First Virtual (with a transaction cost of $0.30) survive?

Safety. Because the systems that are currently running are based on credit cards, they have the same protections for customers and merchants as cards do. The experimental systems and advanced proposals for purely digital money are based on the science of cryptography, whose mathematical foundations seem as sturdy as bedrock. But the rock rests on sand, for it requires the existence of trusted authorities to administer keys, certify credentials, manage the forwarding agents, and so on. How those authorities will be monitored and how failures might be detected is an area for ongoing research.

Privacy. This is one of the most interesting issues, for there is no obvious answer. The balance between individual privacy and collective security has always been a difficult one, regardless of the context. The technical means already exist for assuring excellent privacy in electronic commerce. Whether individuals are willing to pay the cost of such privacy_and whether today's society even understands what all the costs are_remains to be seen. We suspect that privacy will turn out to be very valuable, but it may take an example of flagrant abuse to convince the public of this. For example, until the McCarthy era in U.S. politics, few citizens thought there was any harm in libraries disclosing what books their patrons had borrowed. Now there are laws forbidding librarians from such disclosures, for society has learned the cost of the loss of privacy. We may see a similar pattern in the digital world.

RELATED ARTICLE: RSA's Public-Key Encryption

Nearly all of the electronic commerce schemes proposed for the Internet rely in one way or another upon the public-key encryption system patented by RSA Data Security. A complete mathematical description of the RSA technology is beyond the scope of this newsletter; an excellent article may be found in the August 1979 issue of Scientific American. Here, we will only summarize the main features.

The basic notion is that there are certain mathematical operations that are easy to do but very hard to undo. An example is factorization. It is easy to multiply two prime numbers to form a composite number, but it is very hard to factor a large composite number into its constituent primes. Moreover, prime numbers are thinly scattered among the integers, making the process of guessing at factors rather unrewarding. On the other hand, testing whether a given number is prime is fairly easy, and there is no limit to the number of primes that exist.

In the RSA scheme, encryption keys are large prime numbers, and are always chosen in pairs. (By large, we mean at least a few hundred bits long.) The encoding process uses one of the primes, while the decoding process requires the other prime. However, knowing the encryption key will not help you discover the decryption key. Thus it is possible to publish one of the keys, provided you keep the other one secret.

There are two main uses for a public-key encryption system: sending secret messages and proving your identity. They use the public and private keys in opposite ways:

To send a message that only the intended recipient can decode, you look up his public key in a directory. (On the Internet, you would send a request to a key server.) You encrypt your message with this key and send it. The recipient uses his private key to decode it. Anyone else who sees the encrypted message will not be able to make sense of it.

To prove your identity, you need only create a message that is encrypted with your private key. Anyone can decode this message by using

your public key, but the fact that your public key works shows both who you are and that the message really came from you (because your private key must have been used).

There are several weaknesses in any public-key approach. First, keys must be generated competently and securely. The system would fail if the same keys were issued to two different customers, and the agency that creates the keys must be trusted to keep the secret key secret. Second, when you look up a public key, you must trust the key server to give you the right one. Third, if your secret key is revealed, there must be a mechanism to invalidate the corresponding public key so that others will no longer use it. Sending a message to all key servers would work, provided you trusted someone to keep a correct list of all servers.

RELATED ARTICLE: Smart cards for digital money

The CyberBucks experiment is being conducted on desktop computers, but if e-cash is ever to become a real currency, it will have to be as portable as a credit card. Fortunately, smart cards have already been invented, and are in common use as security tokens. They contain specialized chips for handling complex challenge-response authentication schemes, keypads for entering pin numbers and infrared links for communication with other devices. They are reasonably resistant to chemical attack, probing by x-rays or electron microscopes and other attempts to discover their secrets.

Such a card could be used to store digital money. For example, a simple extension of today's telephone card (which is filled up by a central machine, then gradually emptied as you make phone calls) would allow prestored digital coins. Such cards could be mass-produced in fixed denominations at very low cost, in some estimates as low as $0.10. They would not be rechargeable, but would be thrown away when used up. They could be spent by consuming their coins or by giving the entire card to another person.

Fancier approaches have been proposed for checking the validity of the smart card, preventing duplicate spending of digital coins and so on. Many of them use the concept of a "watcher," a special chip embedded in the smart card that notices, but does not interfere with, all the card's transactions. The watcher can do only one thing: It can respond to a query about whether the card is really authorized to perform a proposed transaction. For example, a watcher circuit could examine the use of digital coins, recording their serial numbers and checking for duplications. If you tried to spend a coin twice, the watcher (if anyone were to interrogate it) would have to admit that the coin had already been spent.

The key issue is how the watcher itself could be shown to be trustworthy. For example, it might contain a self-destruct mechanism to prevent tampering. Fundamentally, however, relying on a watcher is tantamount to relying on the company that makes the chips and embeds them in your smart card.

SPECIAL FEATURES: illustration; other
COMPANY NAMES: CommerceNet--Products; Netscape Communications Corp.--Products
DESCRIPTORS: Internet; Digital Communication; Encryption; Data Security Issue; Database Access Software; Technology Information; Technology Overview
SIC CODES: 7372 Prepackaged software
TRADE NAMES: CyberCash (Database access software)--Design and construction; Netscape Navigator (Database access software)--Design and construction
FILE SEGMENT: CD File 275
?

? t s8/9/3

8/9/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00819310 94-68702

A modern approach to retail accounting

Switzer, Gerald J

Management Accounting v75n8 PP: 55-58 Feb 1994 CODEN: MGACBD ISSN: 0025-1690 JRNL CODE: NAA
DOC TYPE: Journal article LANGUAGE: English LENGTH: 4 Pages
SPECIAL FEATURE: Charts
WORD COUNT: 3053

ABSTRACT: Retailers should use today's computer technology not only to track sales, but also to manage gross margins and control inventory. There is a modern system approach that will accomplish this objective and use item level as a common denominator for the reporting of sales, gross margins, and inventory positions. It combines techniques already in use with some new ideas to create a comprehensive management information system that will provide: 1. immediate information on sales, gross margins, and inventory positions as the day unfolds, 2. immediate accumulation of this information upward to higher management responsibility levels, 3. information to take immediate corrective action when performance is not meeting expectations, 4. the ability to look ahead and plan gross margin targets and inventory levels, 5. gross margin and inventory values that represent the actual sales activity more precisely, and 6. perpetual records of inventory levels and gross margin settings. A discussion of how the system works and its advantages is presented.

TEXT: To say that the retail environment has become tough and highly competitive would provoke a "no kidding!" response from people in that business. To succeed, they must have timely, accurate information. The advent of point-of-sale (POS) systems has resulted from management's need to understand more precisely the nature of sales on a by-item basis and to react more quickly to sales trends. Yet, in many cases, the advanced computer technology that made POS possible is not used to provide this same detailed approach to the crucial areas of sales statistics, gross margin management, and inventory control. It should be!

There's a modern system approach that will accomplish this objective and use item level as a common denominator for the reporting of sales, gross margins, and inventory positions. It combines techniques already in use with some new ideas to create a comprehensive management information system that will provide:

1. Immediate information on sales, gross margins, and inventory positions as the day unfolds.
2. Immediate accumulation of this information upward to higher management responsibility levels.

3. Information to take immediate corrective action when performance is not meeting expectations.

4. The ability to look ahead and plan gross margin targets and inventory levels.

5. Gross margin and inventory values that represent the actual sales activity more precisely.

6. Perpetual records of inventory levels and gross margin settings.

To get a better understanding of the benefits of change, let's look at the way most retailers calculate gross profit and control inventory levels.

The "Retail Inventory Method" is the most common procedure used today. See Table 1. (Table 1 omitted) Opening inventory and purchases are combined with permanent markdowns and markups to determine a cost complement percent. In the retail column, sales are subtracted along with temporary and clearance markdowns to arrive at a "retail" book inventory. Then this number is multiplied by the cost complement percent to arrive at a "cost" book inventory. The "cost" book inventory is subtracted from the "cost" goods available number to arrive at cost of sales. Physical inventory results are included in the retail column with the cost calculated using the same percentage.

This method was necessary in the past because the selling price and the accumulation of sales were the only numbers readily available to the retailer. To cost out individual sales or a physical inventory would require a prohibitive effort considering the number of items involved and the need to go back to invoice costs. Previous computer technologies were inadequate to handle the volume or were prohibitively expensive.

The trade-offs, however, are readily apparent. Under the Retail Inventory Method, inventory value does not reflect actual inventory on hand, and cost of sales does not reflect what actually was sold because the cost complement percent is an average cost-to-retail relationship of all goods available for sale. The calculation also can be misleading because while the dollar value of an inventory may fall within desired limits, the product mix may not be correct. The inventory might consist of a high percentage of old merchandise or items out of season, and this mix will not be apparent to management. Additionally, because markdowns and markups are an integral part of the calculation, that part of shrinkage attributable to mishandling of paperwork increases dramatically and makes determining actual merchandise lost to theft or breakage that much harder to determine.

Because the Retail Inventory Method calculation is done after sales have occurred, and generally on a monthly or sometimes a weekly basis, in today's world it is neither timely nor forward looking and therefore not the best tool for planning.

Computer technology has reached the point where alternatives can be considered and implemented with reasonable cost and ease. The system would be operable on PCs for most retailers and should not require mainframe architecture except in the most complex environments. This system is designed primarily to provide better management controls and does not preclude use of the Retail Inventory Method for outside reporting, if a company still wants to use it.

HOW THIS SYSTEM WORKS

An automated receiver system downloads information to an inventory control database. Automated receiver systems are not new and are used widely by retailers now. Automation of the receiving process is essential to the system to promote accuracy and to eliminate a prohibitive manual effort.

Purchase order data would be downloaded to the receiver system through an automated purchase order system or manually. The key data required from the purchase order would be item code, quantity, cost, freight terms, and discount terms. In most automated receiver applications, selling values are maintained in or can be accessed by the receiver system so would have to be added for new items only. Now the open purchase order data reside in the receiver file pending receipt of the goods.

Upon receipt of the merchandise, quantities received are entered into the receiver system along with the amount of freight charges, if known. Freight can be handled in either of two ways: If the freight charges are known when

a store receives the merchandise, the actual charges can be entered. If freight charges won't be known until a later date, a percentage freight allocation can be calculated automatically, then adjusted periodically based on actual charges incurred. In either event the system would check the freight terms from the purchase order data before accepting any freight charges. Information, including selling value, is provided by the receiver system for label and tag generation and to verify pre-labeled merchandise.

Now the receiving system performs several functions from the data. First, it recalculates the cost of the order based on the actual amounts received and **sends** this information to the accounts payable area for **comparison** with the vendor **invoice** . Accounts payable may be a **store** function or a centralized accounts payable area at regional or corporate offices. Second, the system calculates a "landed cost" by adding or allocating any freight to the item cost. (Imported merchandise would include duty, ocean freight, and commissions also.) Then it downloads item code, date received, quantity received, landed cost, and selling value to the inventory control database, which creates a record of the receipt.

In order to calculate "landed cost" properly, the receiver system must be able to calculate a per-unit freight cost based on the actual or the allocated freight charges. If more than one allocation percentage is desirable to differentiate between high-cost small items and low-cost larger items, the proper allocation percentage would be included as part of the freight terms on the purchase order data downloaded to the receiver system. This real percentage would replace a standard allocation percentage residing in the receiver system.

Merchandise returns to vendors are entered into the receiver system along with any applicable freight charges or credits. Then the system prepares the necessary shipping documents to accompany the merchandise and downloads data concerning the return to the accounts payable area. Additionally, the receiver system updates the inventory control database, which either eliminates or adjusts the inventory record for this shipment depending on whether the return is a partial or entire return. If the return is made long after the store receives the shipment, the original record of shipment no longer may exist. In this case, the quantity returned will be deducted from the current active record for this item.

NOW FOR THE PLANNING MECHANISMS

The inventory control database (see Figure 1) is the heart of the system for controlling gross profit margins and inventory. (Figure 1 omitted.) Based on data received from the receiver system, it establishes a unique record for each shipment received (see Table 2). (Table 2 omitted.) Preferably this function would be online so an employee could look up the most current data on items available for sale, but it may be more practical to have the updates occur several times a day instead.

The point-of-sale system would use the inventory control database to get direct access to retail prices or to spin off the item code and retail prices to a separate file for price lookup if it is more practical. When a sale occurs, the POS system sends the sale information to the inventory control database, which adds cost information and computes the gross profit for each item of that sale and adjusts inventory levels.

Continuing with Figure 1, various standard and ad-hoc reports are available to store management through the sales and gross profit report generator and the inventory report generator, both of which access the database. These reports can be replicated and/or summarized upward to regional and corporate levels.

Table 2 shows the file layout for the inventory control database. It illustrates the concept. In actual implementation, it might contain additional data such as purchase order number and separate freight amounts

to aid in merchandise returns or item location codes if the system is used in a warehouse environment.

Where multiple records exist for the same item, such as item 74101-70750, the active record would be determined by the date received and whether the company chooses a first-in, first-out (FIFO) or last-in, first-out (LIFO) application. If LIFO is chosen, the record with the earliest received date (01/05/93) would be the active record, with the next record (01/19/93) becoming active upon exhaustion of the first record. If FIFO is chosen, the 02/12/93 record would be made active first, followed by the 01/19/93 record. The inventory records are exhausted by entries from the POS system.

Where vendors offer items at a reduced cost in anticipation of a promotional event, the inventory record for those items doesn't have to become active until the event date. Then it would supersede all other records until its exhaustion. This system provides a better matching of cost and selling values during the event. Upon exhaustion of the record or termination of the event, the system would revert to the normal FIFO or LIFO exhaustion process.

As I noted earlier, merchandise returns would be deducted from the active record if the original record of receipt had been exhausted because of the time lag between receipt and return of the item.

CHOOSE THE ADVANTAGES MOST IMPORTANT TO YOU

The advantages of this system are many compared with the Retail Inventory Method. Cost of goods sold now is based on what actually was sold, and the value of inventory represents what actually is on hand. Also, a better matching of sales and costs is possible for promotional events. Information is more timely, and forward-looking analysis is more feasible.
Sales and gross profit is the most important reporting that could be done and can be tailored to satisfy specific business needs. The accumulation of sales and gross profit by item, department, store, district, region, and throughout the company and the availability of this information on a daily, weekly, monthly, and year-to-date basis provide a powerful database from which to derive inquiries on item and location performance.

While standard reports would be generated on a daily, weekly, monthly, and year-to-date basis, the real power of the system is its ability to make inquiries of the data as the day proceeds. This gives management the ability to make decisions and take immediate corrective action.

For example, management could monitor sales results of items that have been relocated to other departments in an attempt to improve sales, or it could monitor the effect of changes in entire aisle and/or department layouts. Corporate inquiries might include how an important sales day is going or the effect on sales of adverse economic occurrences in a particular area, say, due to a plant closing. How are sales of a particular item doing, and which stores are top sellers of that item? Other inquiries based on historical data would be useful in planning promotional events, scheduling employee needs, and the like.
The "hot selling" list, an important tool used in planning purchases, is produced by most companies today using POS data. It is important to identify hot sellers as quickly as possible so orders can be placed to ensure adequate stock. Companies that are slow to discover hot sellers may have difficulty obtaining merchandise and lose sales.

A list of "slow selling" items is less common, but it, too, is important for inventory control. The ability to recognize those items on a timely basis gives management the opportunity to reduce or stop purchases before the items are overstocked.

Gross profit exception reporting would be used to identify items with an incorrect selling price or to gauge the number and/or gross profit effect

of price leaders and profit leaders. Management could request a list of all items under or over a specified gross profit percent, and the sales volumes could be attached to the items if a total effect were desired. Store managers could take corrective action to adjust selling prices immediately, not a week or a month later.

Selling rate in relation to stock-on-hand comparisons will help management determine proper item inventory levels. Comparisons would be based on formulas unique to each company and would have to consider product ordering lead times. Inventory could be shifted to locations with a higher selling rate to reduce overstock positions that may be developing or marked down to move it out.

Sales events, clearances, and other promotional results now can be determined clearly because of the way the data are structured. This information would help management determine the scope and length of future events, the amount of additional store traffic these events generated, and similar selling tips.

Item returns over a predetermined rate also can be identified, which would enable management to remove truly defective items from the shelf and reduce customer dissatisfaction.

NEW INVENTORY REPORTING

Better inventory reporting also is available with this new system. Because inventory data are accumulated by item, department, store, district, region, and company, inquiries into the data have capabilities similar to sales and gross reporting. Inquiries can be made as to the number of items on hand at a specific location, district, region, and the like. How old are those items? What is the current gross margin on those items?
"Old inventory" reporting would be an exception report whereby some or all items that were received prior to a specific date could be listed so management could take immediate corrective action to reduce the quantity of these items. This information is helpful particularly where a company uses a series of planned markdowns to move items as they age. In this case the entire markdown program could be automated.

Gross profit in inventory reporting can provide gross margin dollars or percents for individual items or for the entire store, district, region, or company that currently exists in the inventory on hand. "This tool would be useful in fine-tuning gross margins to enable management to hit a gross margin plan or to know what kind of gross they can expect in the future. Again, corrective action can be taken by adding higher gross merchandise or lowering prices if future sales do not appear to meet targeted gross margins. This ability to look forward is invaluable.

"Overstock/understock" reporting would reveal those locations with too much or too little inventory depending on whether an item is becoming a dog or a new hot seller. It also would be used in conjunction with inventory modeling in more sophisticated applications. Sometimes inventory models are created whereby the ideal inventory mix for a particular store or geographic region of the country is established. Obviously, inventory requirements of stores located in the South may be different from stores located in the North. The models would be run periodically against the inventory control database, and an overstock/understock report would be generated to provide information for inventory adjustments to maintain the optimal mix.

Gross profit exception reporting would enable management to determine those items in inventory above or below a specified gross profit percentage. Corrective action to adjust selling prices where changes are desired could be taken immediately. Management also would have a more comprehensive picture of its gross structure as it relates to loss leaders or high-gross items.

Competitive pricing reporting gives a store manager the ability to enter prices obtained by shopping other stores and to receive a report comparing them with the current prices in his/her store. This report would show the price differences and the effect on gross profit of changing prices to meet the competition based on the current quantities on hand. This feature would be useful particularly where large numbers of competitive price data are compared.

Physical inventory reports would compare physical quantities entered to the current quantities in the inventory control database. Differences shown would trigger recounts and eventual adjustments to the current quantities. Because a perpetual record of all items now exists, physical inventories could be taken on a rotating basis within the store with emphasis on high-value, high-pilferage items. This report would provide more timely discovery of excess loss than a once-a-year or twice-a-year inventory and would allow for quicker action to reduce the losses. Additionally, scheduled rotating inventories can eliminate the need to shut down a store for physical inventories and would provide shrinkage information throughout the year for planning purposes.

Finally, now the ability to look forward and know the cost of running clearance items is possible. While clearing out the item may be a foregone conclusion, the effect on gross profit can be determined ahead of the final sale. Also, the effect of running certain types of inventory reduction promotions can be determined before they are run so that targeted gross margins for the event can be maintained. As with the sales and gross reporting, inventory reporting requirements can be tailored to the particular business needs of the company.

Retailers need every advantage possible in today's tough market. No system can replace management's good judgment, but the system I described does present powerful tools that will help management in monitoring current performance, planning for the future, and providing early warning signals of negative future trends. While it cannot replace proper buying disciplines or predict unforeseen economic events, it can provide a competitive edge through advanced technology that is available now.

Gerald J. Switzer has spent 20 years in retailing. Formerly with Kmart Corporation, he held numerous financial positions there including corporate controller. He is a member of the Detroit Chapter, through which this article was submitted, and can be reached at (313) 645-2494.

GEOGRAPHIC NAMES: US

DESCRIPTORS: Management accounting; Retailing industry; Inventory control; Inventory costing methods; Financial management; Automated accounting systems; Advantages
CLASSIFICATION CODES: 9190 (CN=United States); 4120 (CN=Accounting policies & procedures); 8390 (CN=Retailing industry); 5330 (CN=Inventory management); 3100 (CN=Capital & debt management); 5240 (CN=Software & systems)
?

? t s12/9/135

12/9/135 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

00628337 CMP ACCESSION NUMBER: EBN19890612S1106
The Impact Of EDI
Stephen P. Kaufman
ELECTRONIC BUYERS' NEWS, **1989** , n 654, 15
PUBLICATION DATE: 890612
JOURNAL CODE: EBN LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: EDITORIAL
WORD COUNT: 772
TEXT:

Myths and confusion abound as to what electronic data interchange (EDI) is and how it will affect our industry.

Every year, it seems, a new concept is heralded as the solution to restoring America's competitive edge. This year, it's electronic data interchange (EDI).

The electronic purchasing community is being hit with a tidal wave of sales literature claiming that EDI will help simplify all the administrative aspects of the ordering process. In fact, true EDI can do this, but myths and confusion abound as to what EDI is and how it will affect our industry.

Contrary to some beliefs, EDI does not consist of in-plant terminals or electronic mailboxes. It does not involve a purchaser looking at an order, requesting a quote, writing an order or processing one. There are no messages to be read, acted upon or approved.

Strictly defined, EDI is the electronic interchange of standard business documents without human intervention. Since EDI's appearance several years ago, the "paperless transaction" has become a reality. With EDI, a purchaser enters a bill of materials into his own company's computer system, and his and the supplier's computers do the rest. The customer's computer checks the supplier's inventory, pricing and delivery schedules and processes the order. The supplier's **computer** acknowledges the order, **sends confirmation** of delivery and **sends** an **invoice** and **receives** payment automatically.

The benefits are obvious: increased speed and accuracy, administrative simplification and closer partnership. Compared with the cost of a hard copy purchase order, the electronic PO can save more than 50%. And the efficiency makes it ideal for JIT programs.

If it sounds expensive, it is. The initial investment in EDI technology can range from hundreds of thousands of dollars to millions , which is why the charge is being led by the biggest, most profitable organizations, such as AT&T Co. and Hewlett-Packard Co.

Undoubtedly, EDI will have a major impact on our industry. Technological advances aimed at simplification often affect business in surprising ways. For example, the word processor increased the productivity of the typing pool, as promised. But since it is now so easy to retype a page, the time spent revising, redrafting and polishing documents often equals or surpasses the time previously spent typing them. So there is little, if any, reduction in the number of secretaries or typists employed.

What is EDI likely to contribute and what side effects can we anticipate?

Currently, EDI is creating four dimensions of change. The first is time. The process of ordering, acknowledging, billing and paying is done in seconds without human intervention. Therefore, telephone tag, lost purchase orders, lag time and other delays are eliminated.

The second dimension is accuracy. Errors due to typos, transpositions of numbers, language misunderstandings and inattentive

personnel become a thing of the past. In addition, EDI users have several systems of verification to choose from to evaluate every transaction and quickly identify mistakes.

The third dimension is administrative simplification. Once computers are handling many of the clerical tasks associated with procurement, companies could have lowered administrative costs, thus making it possible for purchasing professionals to focus on other issues, such as quality improvements, long-range supplier planning, design of performance tracking systems and negotiations of major contracts.

The fourth dimension is the most complex and the hardest to anticipate. EDI is changing the relationship between customer and supplier and dramatically altering the roles of purchaser and salesperson. Purchasers will have more time for long-term considerations, such as sourcing, value-added service requirements and future product developments. Sales representatives will spend less time with purchasing people and more time with engineers. In this new role, they will have to become more technically oriented in order to help engineers formulate new designs that integrate a vast range of suppliers' products.

The expense of EDI will force customers to reduce their vendor bases even further. As customers and suppliers set up their data links and long-term buying relationships, legal agreements will have to clarify commitments, pricing formulas and profits. But will these closer partnerships lead to source loyalty or simply automate the erosion of profit margins, thus accelerating the failures, exits and consolidations that have reduced the ranks of distributors during the past decade?

EDI will solve some problems and simultaneously create a new set of challenges at every level of involvement. If we work together to anticipate and plan for change now, we can use EDI to simplify the purchasing process and create stronger, healthier relationships between customers and suppliers.

Stephen P. Kaufman is president and CEO of Arrow Electronics Inc.

?

? t *s12/9/20*

12/9/20 (Item 11 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00975883 96-25276

Completing the loop

Garry, Michael

Progressive Grocer v74n2 PP: 75-80 Feb 1995 ISSN: 0033-0787
JRNL CODE: PGR
DOC TYPE: Journal article LANGUAGE: English LENGTH: 3 Pages
SPECIAL FEATURE: Charts
WORD COUNT: 1233

ABSTRACT: While the goal of paperless information flow has so far remained largely outside the realm of most grocers, at least one - 156-store Giant Food - has recently implemented a chainwide direct store delivery (DSD) system with 2 vendors (Nabisco and Frito-Lay) that is driven solely by electronic data interchange (EDI). James Peterson, Giant's director of systems research, calls the new system a significant achievement that completes the loop - electronically covering all phases of a DSD transaction from order through payment. What makes Giant's system significant is that it eliminates 2 of the main sources of error in the DSD process - paper and people.

TEXT: One of the cherished goals of the efficient consumer response (ECR) initiative is paperless information flow --replacing paper with electronic data interchange (EDI). While that goal has so far remained largely outside the realm of most grocers, at least one--156-store Giant Food, Landover, Md.--has recently implemented a chainwide direct store delivery (DSD) system with two vendors (Nabisco and Frito-Lay) that is driven solely by EDI.

James Peterson, Giant's director of systems research, calls the new system "a significant achievement" that "completes the loop"--electronically covering all phases of a DSD transaction from order through payment. The Giant project is one of the few--if not the only one--of its kind in the industry.

Giant's DSD project was one of the pilot efforts conducted by the integrated EDI work group, part of the ECR best practices operating committee. Another work group, the DSD Holistic Pilot Project, has just released a report that includes Giant's DSD program.

(For 16 other vendors, Giant has not "completed the loop" as it has with Nabisco and Frito-Lay, but has begun the process by replacing paper invoicing with direct exchange of electronic information at the back door, called DEX/UCS.)
What makes Giant's system significant is that it eliminates two of the main sources of error in the DSD process--paper and people. By using DEX with 18 vendors, Giant has eliminated some 450,000 paper invoices annually, says Peterson. By adding another six vendors to the DEX band-wagon in 1995, Giant hopes to get rid of another 300,000 paper invoices. The elimination of so many paper invoices naturally cuts back the clerical labor needed to enter data.

Over time, says Peterson, by removing paper and clerical labor in DSD, the billing process becomes more accurate, helping to reduce squabbles over invoice deductions. It's still too early, however, to get a firm read on the effect on invoice deductions, he says. With improved accuracy also come fewer proof-of-delivery problems.

The new Giant system encompasses electronically all of the elements that go into a DSD transaction. For example, product authorization/deauthorization is transmitted to the vendor and entered into the vendor's database.

When the vendor creates an order for Giant, it is compared with the authorized/deauthorized item list. Then the delivery is made to the back door at the **stores** , where the **invoice** is again electronically **compared** with an authorized/deauthorized list and then **transmitted** to the **store** 's computers (the DEX/UCS process).

At the end of the day, all invoices are transmitted from the stores to Giant's headquarters, where they are processed overnight. Once a week the chain transmits to vendors an electronic remittance advice--a statement that tells the vendor what will be paid for and points out any discrepancies between Giant's records and those of the vendor. Finally Giant proceeds with electronic funds transfer (EFT), transmitting payments directly to a vendor's bank.

Peterson says he expects to complete a closed DSD loop with Coca-Cola by mid-1995 and to bring other vendors into the program this year. The more vendors (and retailers) engaged in paperless communications, the greater the payback to each of the participants, he notes. Peterson considers bringing on new participants to be one the major hurdles facing Giant; the other is the software work needed to integrate all EDI transactions into its database so that no manual entry is needed.

In addition to DSD information. Giant also electronically receives at headquarters from selected brokers promotion announcements and price changes, two of the three transactions under what is called UCS II, and integrates them into its database. The other UCS II transaction set--item maintenance--will be accepted and integrated sometime in 1995, says Peterson. Giant, which participated in the original UCS II pilot, is one of the few grocery companies making real progress with UCS II (see sidebar).(Sidebar omitted)

So far, says Peterson, Giant is receiving the promotion and price change information in varying degrees from five brokers; some are in production, others are still testing. Since each broker represents 40 to 70 manufacturers, brokers "are the key to reaching critical mass," he says. If six brokers were in a production mode, Giant would have taken a big step toward critical mass, according to Peterson. In some cases, Giant is receiving the information directly from manufacturers.

How does Giant benefit from receiving promotion and pricing data electronically? As in the DSD program, the aim is to reduce invoice deductions, which result from manual entry of data in paper-based transactions. Manual operations lead to "a lot of confusion and lost data," says Peterson. However, it is too early for him to gauge the exact effect on invoice deductions. In any event, buyers, who were often the ones saddled with manually entering promotion announcements, "are now able to do more important things," he says.
Another plus is that promotional opportunities are not missed when they are communicated electronically. They are presented on-line to buyers, who must react to them. "Paper documents can be overlooked or missing, and not introduced to the system," says Peterson.

Supervalu making strides

Another EDI leader in the grocery industry has been Supervalu, Eden Prairie, Minn., which has been working on the UCS II transactions for several years. (See "UCS II: Breaking through?" Progressive Grocer, April 1993.) Currently Supervalu is accepting promotion announcements (including dates, UPCs and rates) on-line at all of its divisions except for those acquired from Sweet Life and Wetterau, says Greg Zwanziger, EDI/UCS manager for Supervalu. Price changes, which have been accepted by Supervalu for

years, are still being integrated for on-line acceptance. Supervalu hopes to roll out item maintenance by the fourth quarter of 1995.

The largest amount of EDI activity is taking place in Supervalu's Minnesota division, to which some 30 brokers and a dozen manufacturers are transmitting promotion announcements. About 40% of all promotion announcements are communicated by EDI. Brokers, for whom software handling UCS II transactions is available, were a prime target for Supervalu in its efforts to develop EDI trading partners in this division.

As a result of receiving promotion announcements, Supervalu has been able to eliminate invoice deductions by as much as 80% for specific vendors, says Zwanziger. This reduction in deductions also creates a "huge labor savings," he says. Overall, UCS II transactions ensure that information is getting through to Supervalu's retail customers. "In a manual environment, things slip through the cracks and we don't always see promotions and price changes on every item on a timely basis," says Zwanziger.

While EDI generally takes place between suppliers and warehouses, Supervalu is even testing EDI communications from its headquarters to a retail chain.

One of the impediments to receiving promotion announcements via EDI concerns timing. "In the EDI world," says Zwanziger, "some manufacturers are not willing to give out promotions as far in advance as they do under a manual system." Others, like Pillsbury, have given their sales force control over when promotions are released--a scenario that is "far enough in advance for us," says Zwanziger.

And some grocery companies that receive promotion announcements electronically still find the same complexity and uncertainty over timing that have plagued vendor/distributor relations in the past, says David Manigold, partner, Deloitte & Touche, Dallas.

Most of the cost associated with EDI comes from integrating EDI transmissions into buying systems. But once Supervalu is implementing EDI at all of its divisions to the extent that it is at its Minnesota division, "that should easily pay for implementation," says Zwanziger.

COMPANY NAMES:
Giant Food Inc (DUNS:00-691-9757 TICKER:GFSA)
GEOGRAPHIC NAMES: US

DESCRIPTORS: Grocery stores; Case studies; Efficient consumer response; Electronic data interchange; Distribution planning; Information management
CLASSIFICATION CODES: 9190 (CN=United States); 8390 (CN=Retailing industry); 9110 (CN=Company specific); 5250 (CN=Telecommunications systems); 5330 (CN=Inventory management)
?